IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) An encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption, the apparatus comprising:

a plurality of round processing circuits connected in series, the round processing circuit of a first stage receiving a common key and subjecting the received common key to a round function to output a sub key and the round processing circuit of ~~other~~ subsequent stages receiving the sub key output from the round processing circuit of a previous stage and subjecting the sub key to a round function to output a sub key, the sub key output from the round processing circuit of a last stage being the common key; and

a plurality of expanded key generating circuits configured to receive the sub keys output from at least a part of said round processing circuits and output expanded keys based on all or some bits of the received sub keys, wherein the plurality of round processing circuits comprise at least a pair of round processing circuits having inverse round functions.

2. (Original) The encryption apparatus according to claim 1, wherein said plurality of expanded key generating circuits subject the all or some bits of the received sub keys to a predetermined conversion processing to output the expanded keys.

3. (Original) The encryption apparatus according to claim 1, wherein the round function of the round processing circuit of i-th stage is an inverse function of the round function of the round processing circuit of (j-i+1)-th stage, j being an half of the total number of stages of round processing circuits and i being 1 to j.

4. (Canceled)

5. (Canceled)

6. (Original) The encryption apparatus according to claim 1, further comprising a selector configured to select some of the sub keys output from said plurality of round processing circuits, the selected sub keys being supplied to said plurality of expanded key generating circuits.

7. (Original) The encryption apparatus according to claim 6, wherein said selector selects the sub keys output from round processing circuits other than a first group of round processing circuits including the round processing circuit of the first stage and a second group of round processing circuits including the round processing circuit of the last stage.

8. (Original) The encryption apparatus according to claim 6, wherein said selector selects one of the sub key output from a round processing circuit of i-th stage and the sub key output from a round processing circuit of (j-i+1)-th stage, j being an half of the total number of stages of the round processing circuits and i being 1 to j.

9. (Original) The encryption apparatus according to claim 1, wherein said plurality of expanded key generating circuits change an order of the sub keys generated from said plurality of round processing circuits and generates the expanded keys in a changed order.

10. (Original) The encryption apparatus according to claim 1, wherein said plurality of expanded key generating circuits generate the expanded keys in number exceeding the number of expanded keys required for the data randomizing process and output an expanded common key indicating which expanded keys are supplied to the data randomizing process.

11. (Currently Amended) A decryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption, the apparatus comprising:

a plurality of round processing circuits connected in series, the round processing circuit of a first stage receiving a common key and subjecting the common key to a round function to output a sub key and the round processing circuit of ~~other~~ subsequent stages receiving the sub key output from the round processing circuit of a previous stage and

subjecting the sub key to a round function to output a sub key, the sub key output from the round processing circuit of a last stage being the common key; and

a plurality of expanded key generating circuits configured to receive the sub keys output from at least a part of said round processing circuits and output expanded keys based on all or some bits of the received sub keys, wherein the plurality of round processing circuits comprise at least a pair of round processing circuits having inverse round functions.

12. (Original) The decryption apparatus according to claim 11, characterized in that said plurality of expanded key generating circuits subject the all or some bits of the received sub keys to a predetermined conversion processing to output the expanded keys.

13. (Currently Amended) An expanded key generation apparatus used for an encryption apparatus including a data randomizing process using a plurality of expanded keys in a predetermined order and a decryption apparatus including a data randomizing process using the plurality of expanded keys in a reversed order which are based on a common key encryption system, the apparatus comprising:

a plurality of round processing circuits connected in series, the round processing circuit of a first stage receiving a common key and subjecting the common key to a round function to output a sub key and the round processing circuit of ~~other~~ subsequent stages receiving the sub key output from the round processing circuit of a previous stage and subjecting the sub key to a round function to output a sub key, the sub key output from the round processing circuit of a last stage being the common key; and

a plurality of expanded key generating circuits configured to receive the sub keys output from at least a part of said round processing circuits and output expanded keys based on all or some bits of the received sub keys, wherein the plurality of round processing circuits comprise at least a pair of round processing circuits having inverse round functions.

14. (Original) The expanded key generation apparatus according to claim 13, wherein said plurality of expanded key generating circuits subject the all or some bits of the received sub keys to a predetermined conversion processing to output the expanded keys.

15. (Currently Amended) An expanded key generation method used for an encryption apparatus based on a common key encryption system in which a plurality of expanded keys

are used in a predetermined order in a data randomizing process for encryption in a reversed order in a data randomizing process for decryption, the method comprising:

subjecting a received common key to a round function to output a sub key by a round processing circuit of a first stage;

subjecting the sub key output from the round processing circuit of a previous stage to a round function to output a sub key by round processing ~~circuit~~ circuits of ~~other~~ subsequent stages, the round processing circuits of the subsequent stages comprising at least a pair of round processing circuits having inverse round functions, the sub key output from the round processing circuit of a last stage being the common key; and

generating expanded keys based on all or some bits of the sub keys from a plurality of round processing circuits.

16. (Currently Amended) An expanded key generation method used for a decryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption, the method comprising:

subjecting a received common key to a round function to output a sub key by a round processing circuit of a first stage;

subjecting the sub key output from the round processing circuit of a previous stage to a round function to output a sub key by round processing ~~circuit~~ circuits of ~~other~~ subsequent stages, the round processing circuits of the subsequent stages comprising at least a pair of round processing circuits having inverse round functions, the sub key output from the round processing circuit of a last stage being the common key; and

generating expanded keys based on all or some bits of the sub keys from a plurality of round processing circuits.

17. (Currently Amended) An article of manufacture comprising a computer usable medium having an expanded key generation program embodied therein, the expanded key generation program used for an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption, the program comprising:

computer readable program code means for causing a computer to subject a common key to a round function to output a sub key of a first stage;

computer readable program code means for causing a computer to subject the sub key of a previous stage to ~~a~~ round ~~function~~ functions to output ~~a~~ sub ~~key~~ keys of ~~other~~ subsequent stages, the round functions of the subsequent stages comprising at least a pair of inverse round functions, the sub key of a last stage being the common key; and

computer readable program code means for causing a computer to generate expanded keys based on all or some bits of the sub keys.

18. (Currently Amended) An article of manufacture comprising a computer usable medium having an expanded key generation program embodied therein, the expanded key generation program used for a decryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption, the program comprising:

computer readable program code means for causing a computer to subject a common key to a round function to output a sub key of a first stage;

computer readable program code means for causing a computer to subject the sub key of a previous stage to ~~a~~ round ~~function~~ functions to output ~~a~~ sub ~~key~~ keys of ~~other~~ subsequent stages, the round functions of the subsequent stages comprising at least a pair of inverse round functions, the sub key of a last stage being the common key; and

computer readable program code means for causing a computer to generate expanded keys based on all or some bits of the sub keys.

19. (New) The encryption apparatus according to claim 1, wherein the plurality of round processing circuits comprise a first half of round processing circuits and a second half of round processing circuits, a round function of the first half of round processing circuits being inverse to a round function of the second half of round processing circuits.

20. (New) The encryption apparatus according to claim 1, wherein the plurality of round processing circuits comprise a first half of round processing circuits and a second half of round processing circuits, round functions of the first half of round processing circuits being inverse to round functions of the second half of round processing circuits.

21. (New) The encryption apparatus according to claim 1, wherein each of the round processing circuits in the pair of round processing circuit having inverse round functions, comprises logic elements and a plurality of output terminals, such that the plurality of output terminals are connected to different logic elements so that different sub keys are output from each output terminal.

22. (New) The encryption apparatus according to claim 1, wherein each of the round processing circuits in the pair of round processing circuits having inverse round functions, comprises corresponding logic elements wherein the logic elements of each round processing circuit are interconnected differently, so as to output different sub keys.

23. (New) The decryption apparatus according to claim 11, wherein the plurality of round processing circuits comprise a first half of round processing circuits and a second half of round processing circuits, a round function of the first half of round processing circuits being inverse to a round function of the second half of round processing circuits.

24. (New) The decryption apparatus according to claim 11, wherein the plurality of round processing circuits comprise a first half of round processing circuits and a second half of round processing circuits, round functions of the first half of round processing circuits being inverse to round functions of the second half of round processing circuits.

25. (New) The decryption apparatus according to claim 11, wherein the pair of round processing circuits having inverse round functions comprise logic elements and output different sub keys from different terminals connected to different logic elements.

26. (New) The decryption apparatus according to claim 11, wherein the pair of round processing circuits having inverse round functions comprise logic elements connected to each other in a different manner to output different sub keys.